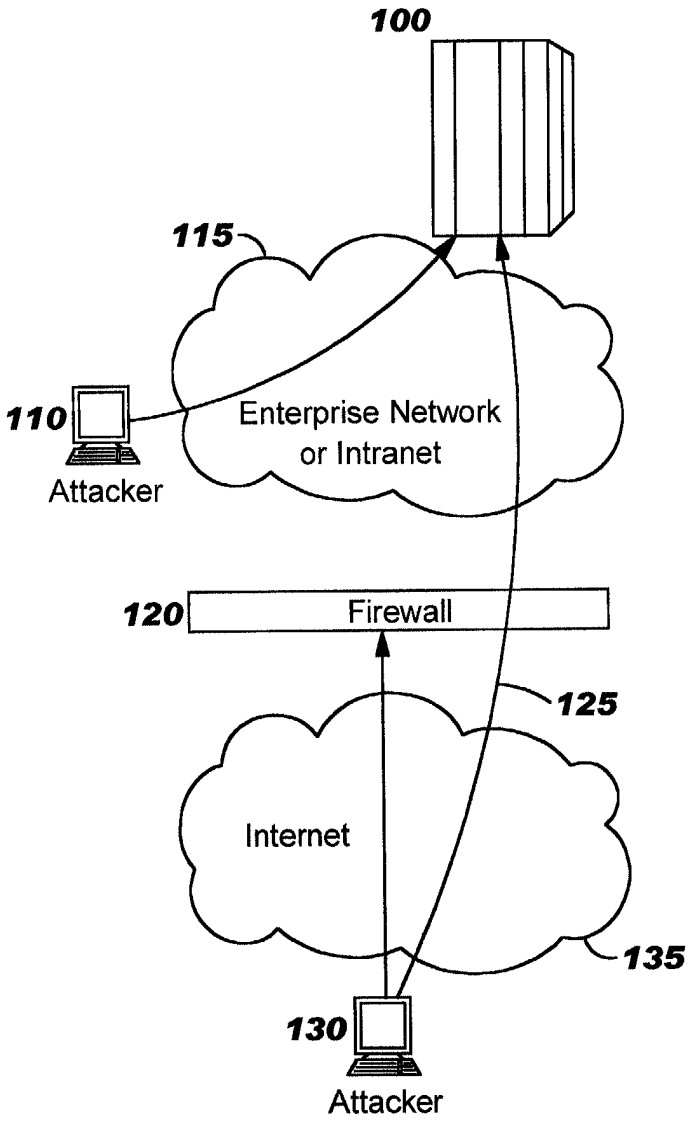


FIG. 1
(Prior Art)

FIG. 2
(Prior Art)

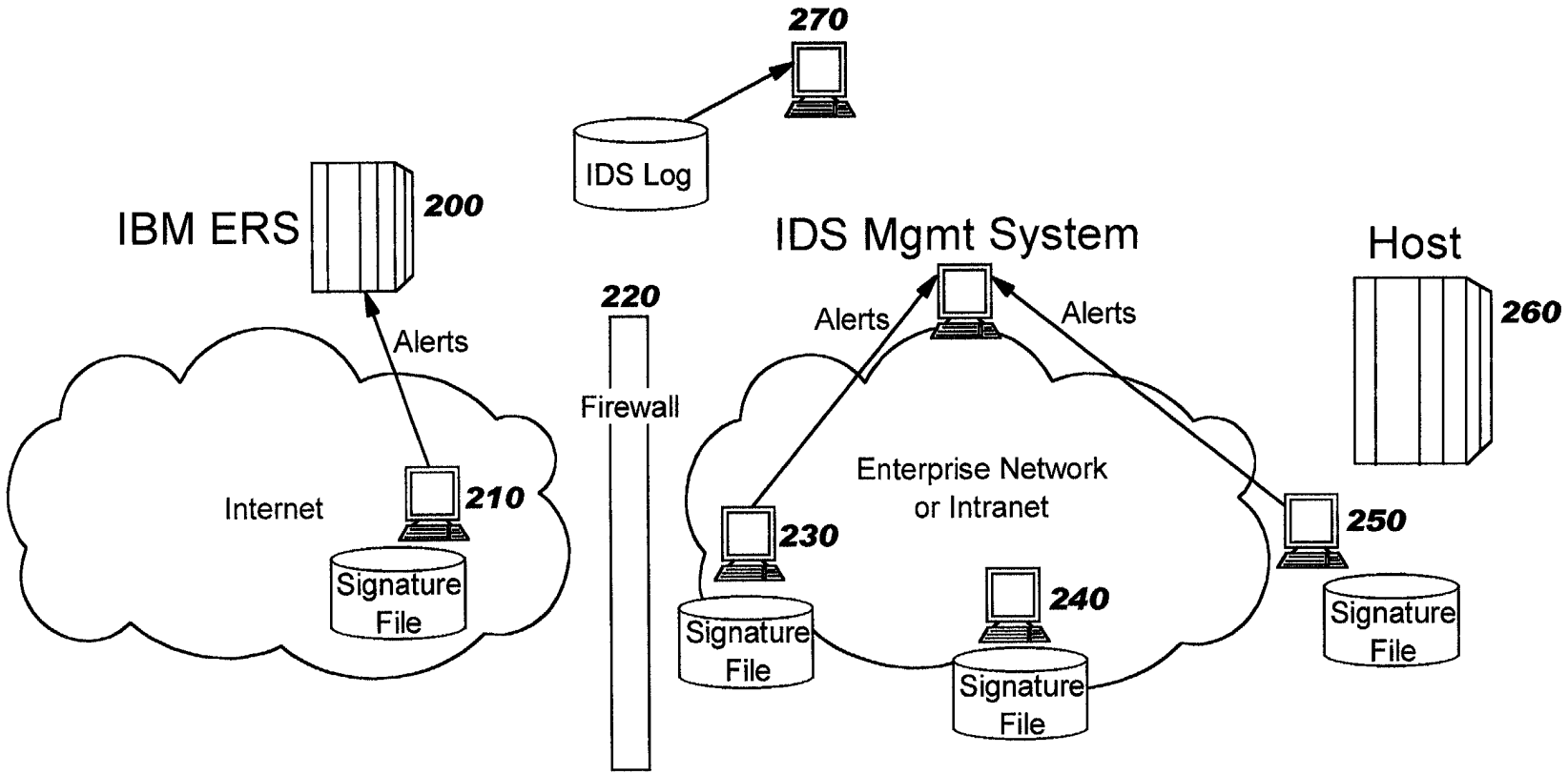


FIG. 3

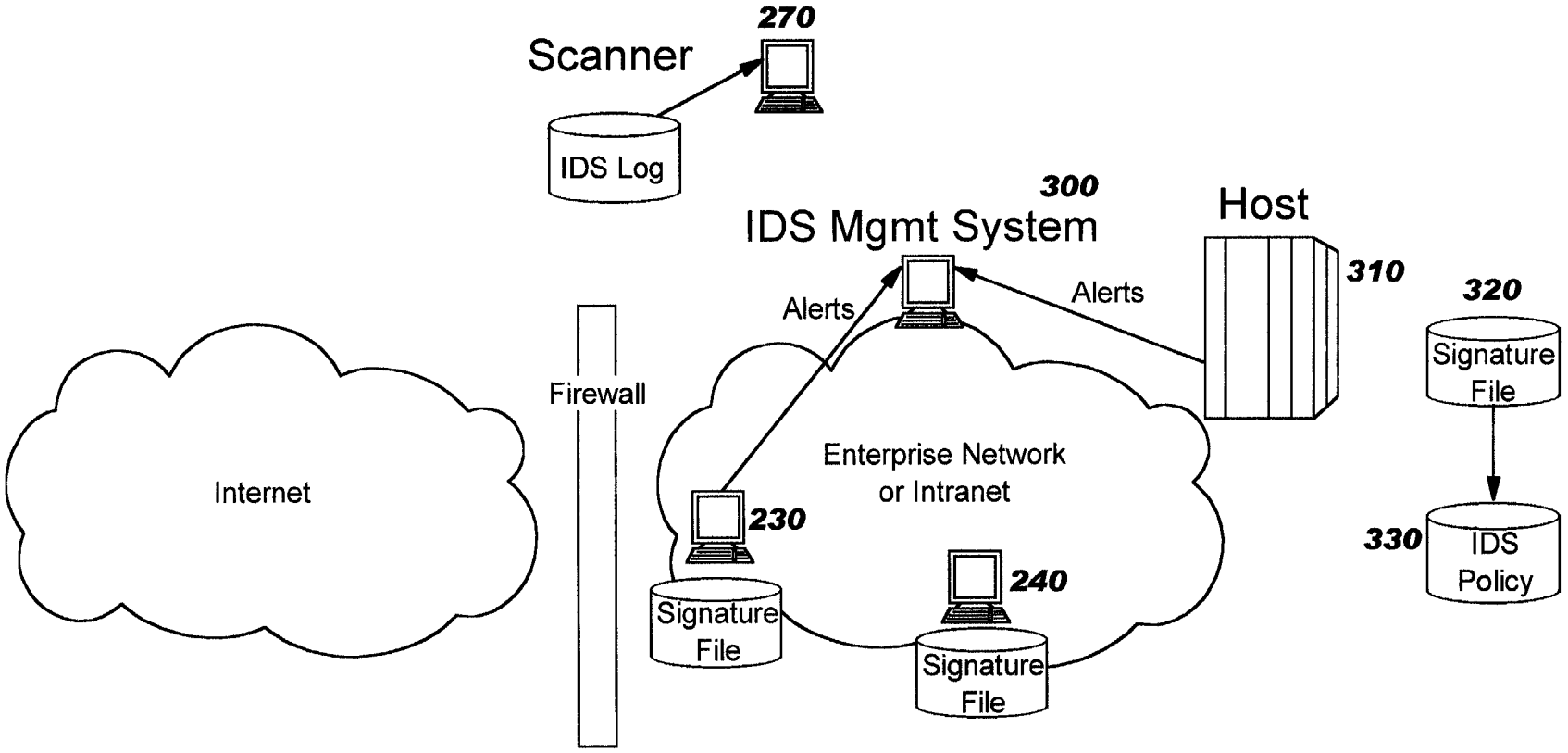

Scanner
270
IDS Log
300
IDS Mgmt System
Host
310
320
Alerts
Alerts
Signature File
Firewall
Internet
Enterprise Network or Intranet
230
240
330
IDS Policy
Signature File
Signature File

FIG. 4

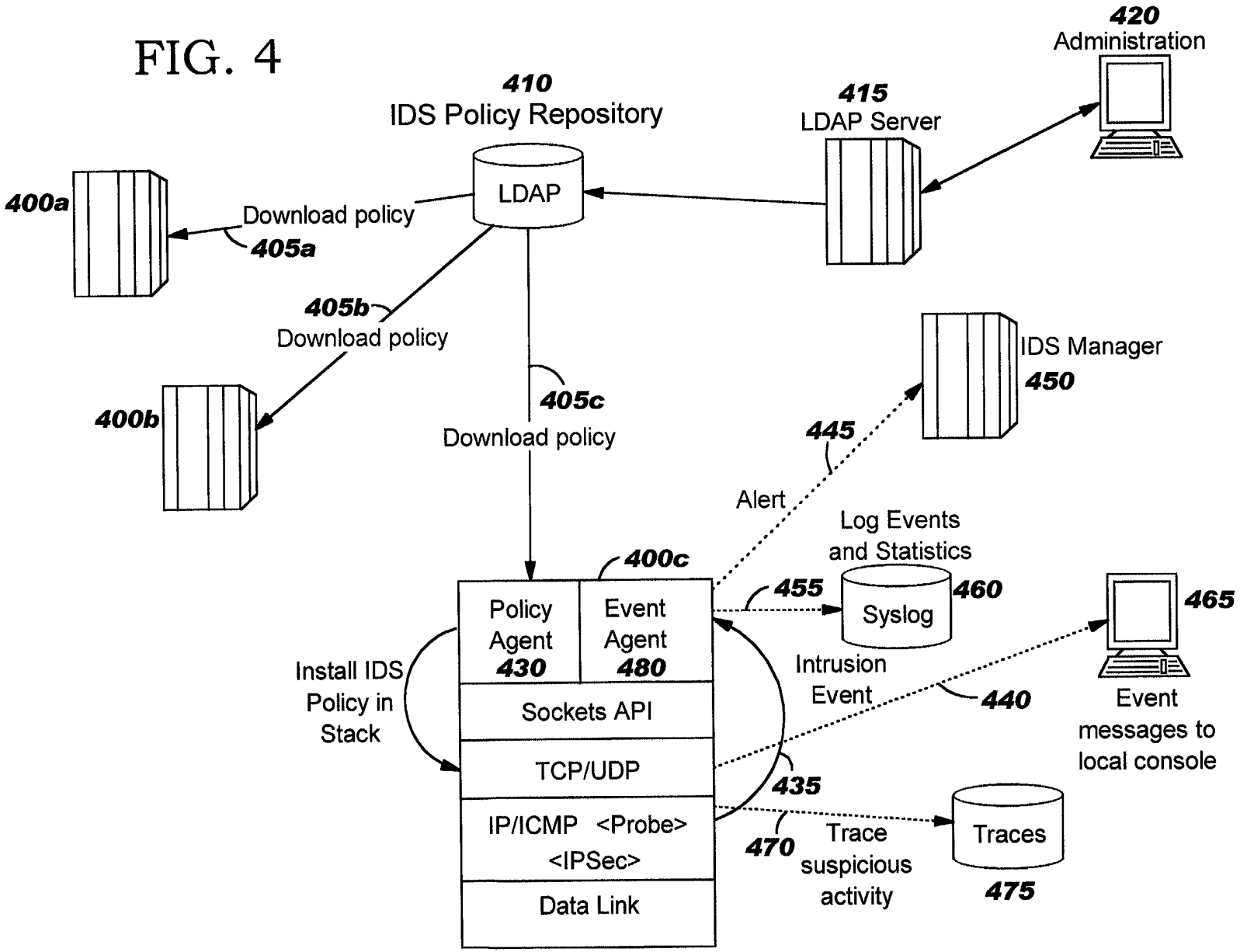


FIG. 5

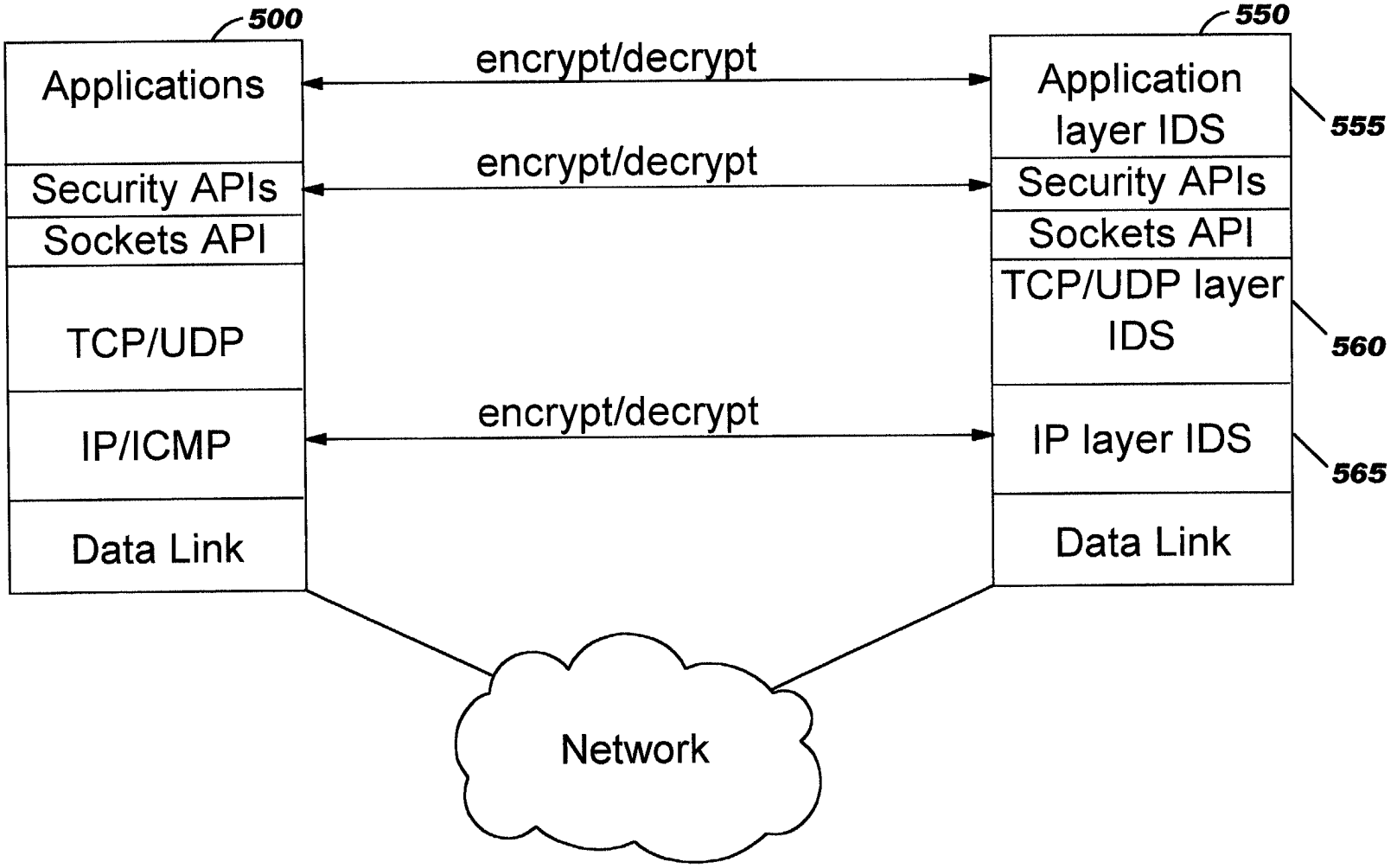


FIG. 6

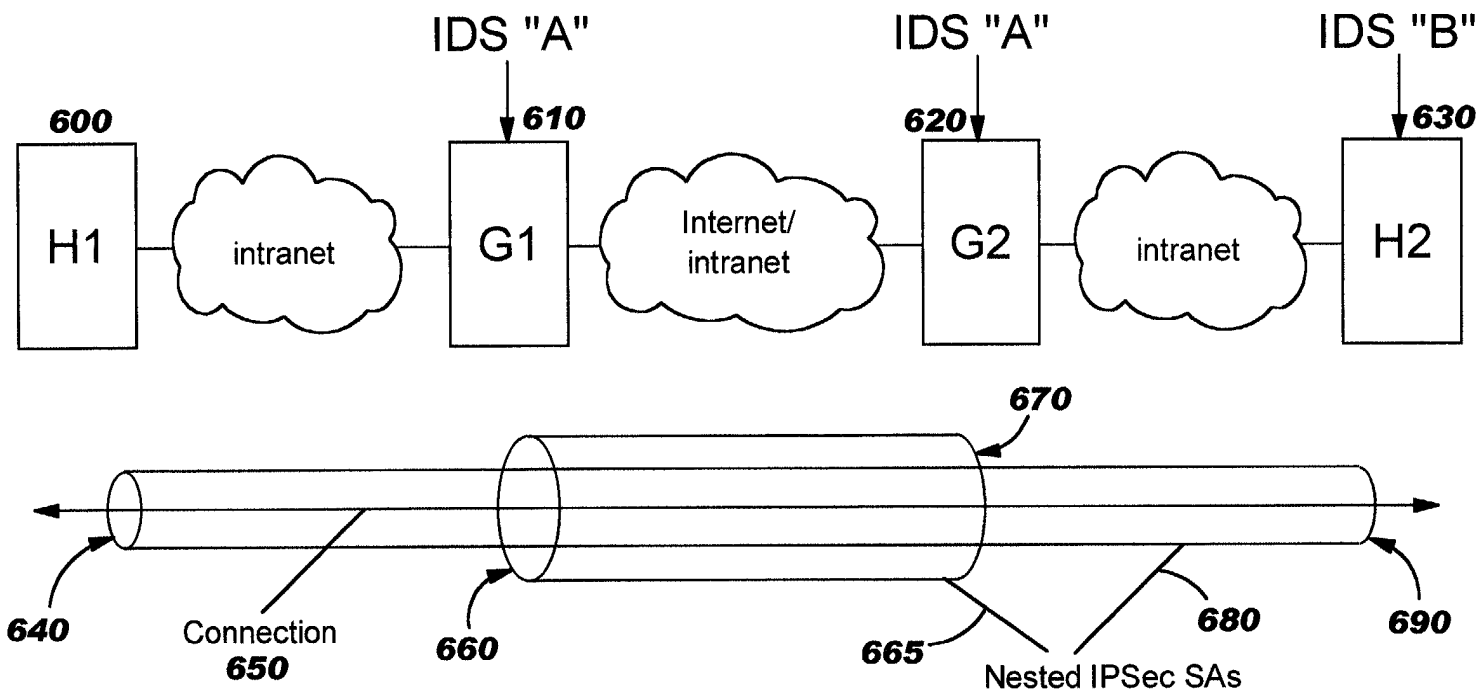

IDS "A"
IDS "A"
IDS "B"
600
610
620
630
H1
intranet
G1
Internet/
intranet
G2
intranet
H2
670
640
Connection
650
660
665
680
690
Nested IPSec SAs

FIG. 7
(Prior Art)

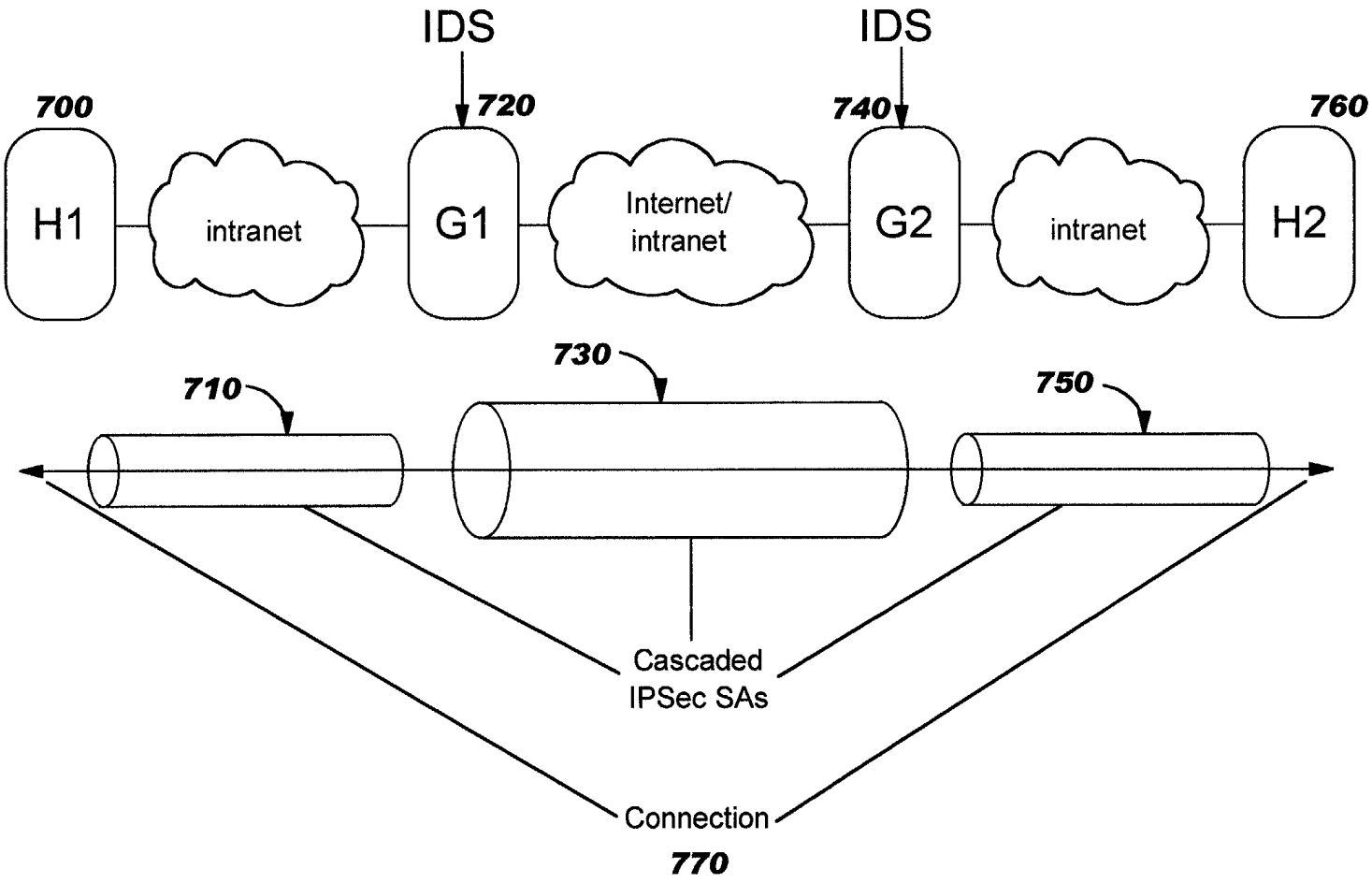


FIG. 8
(Prior Art)

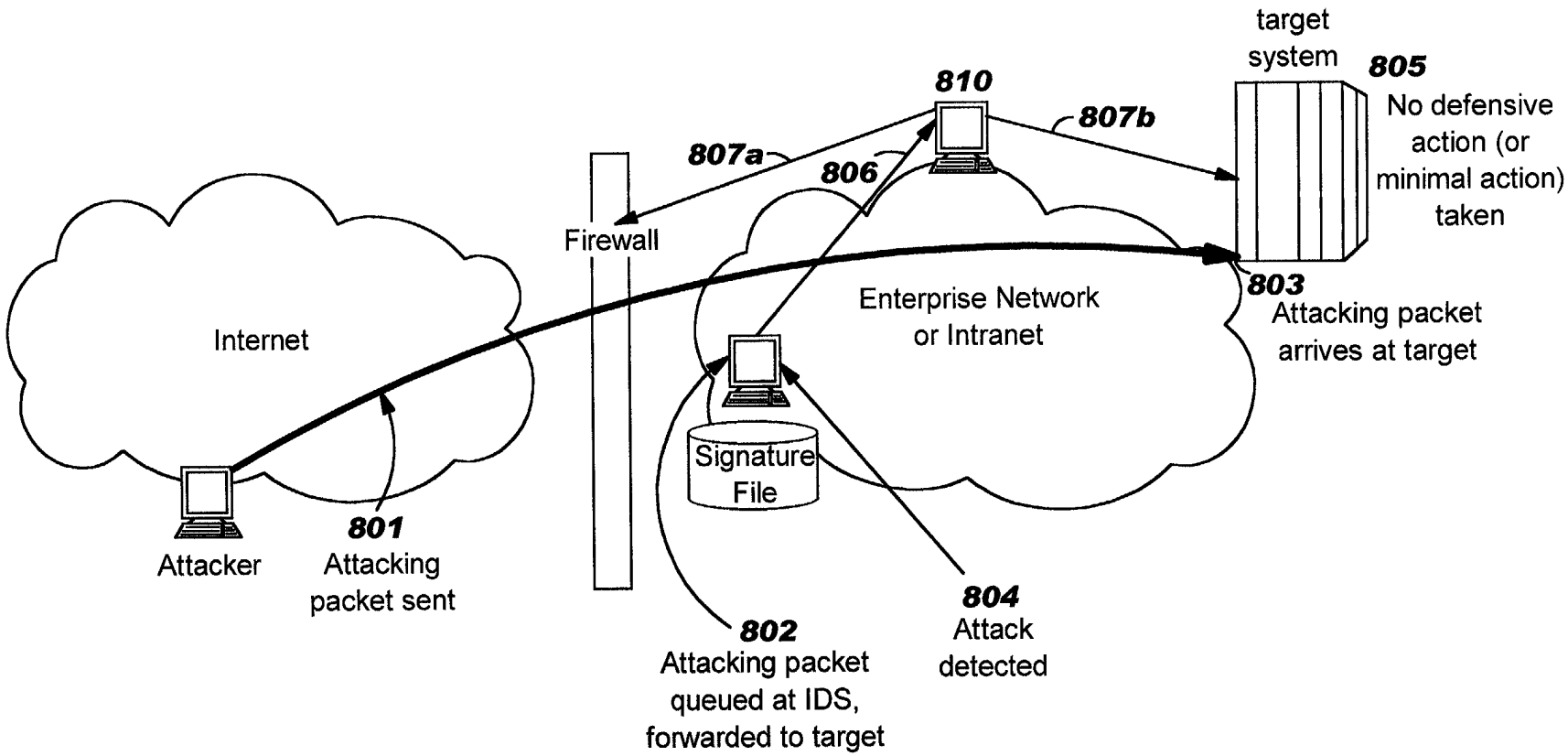


FIG. 9

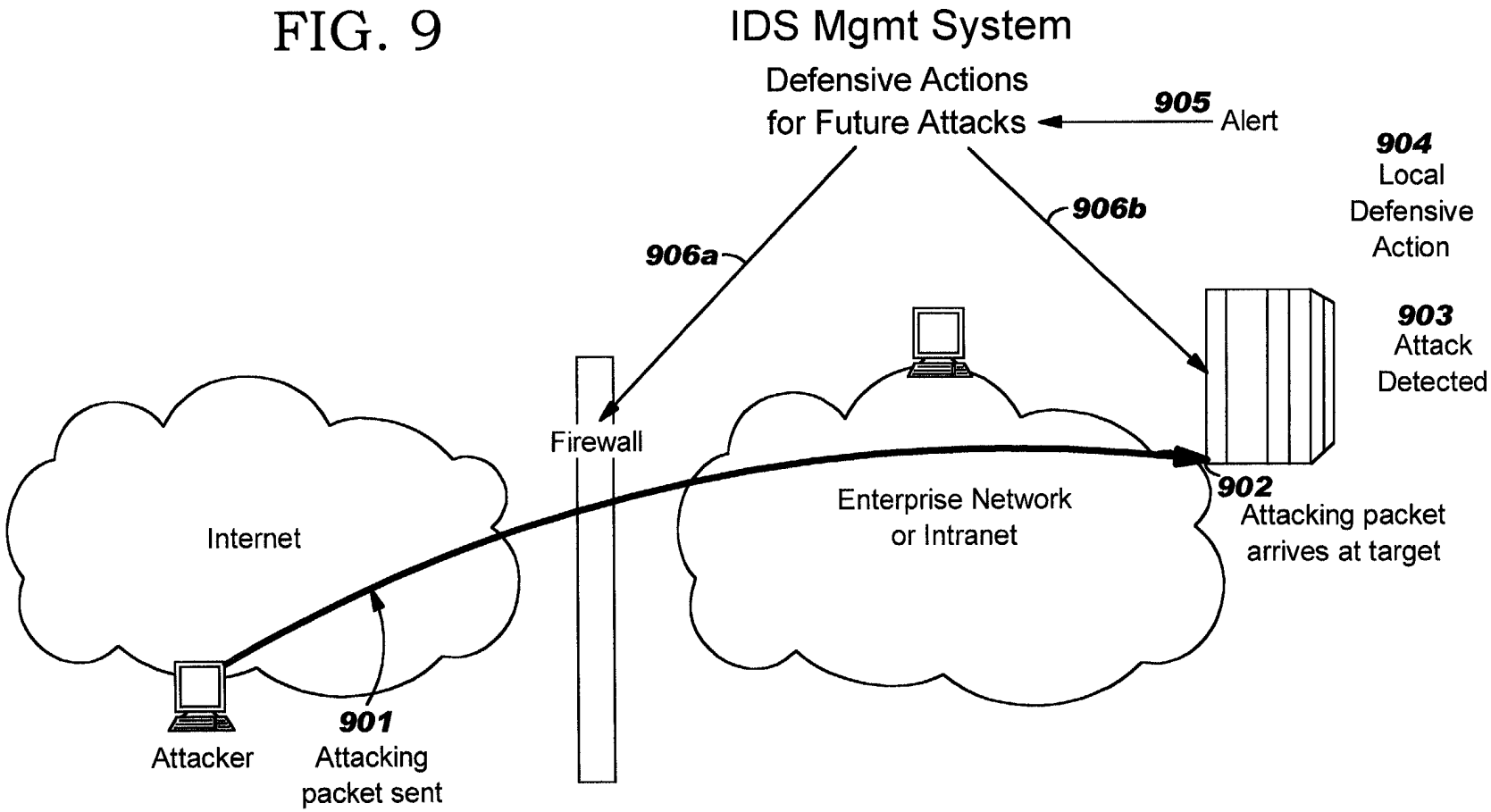


FIG. 10

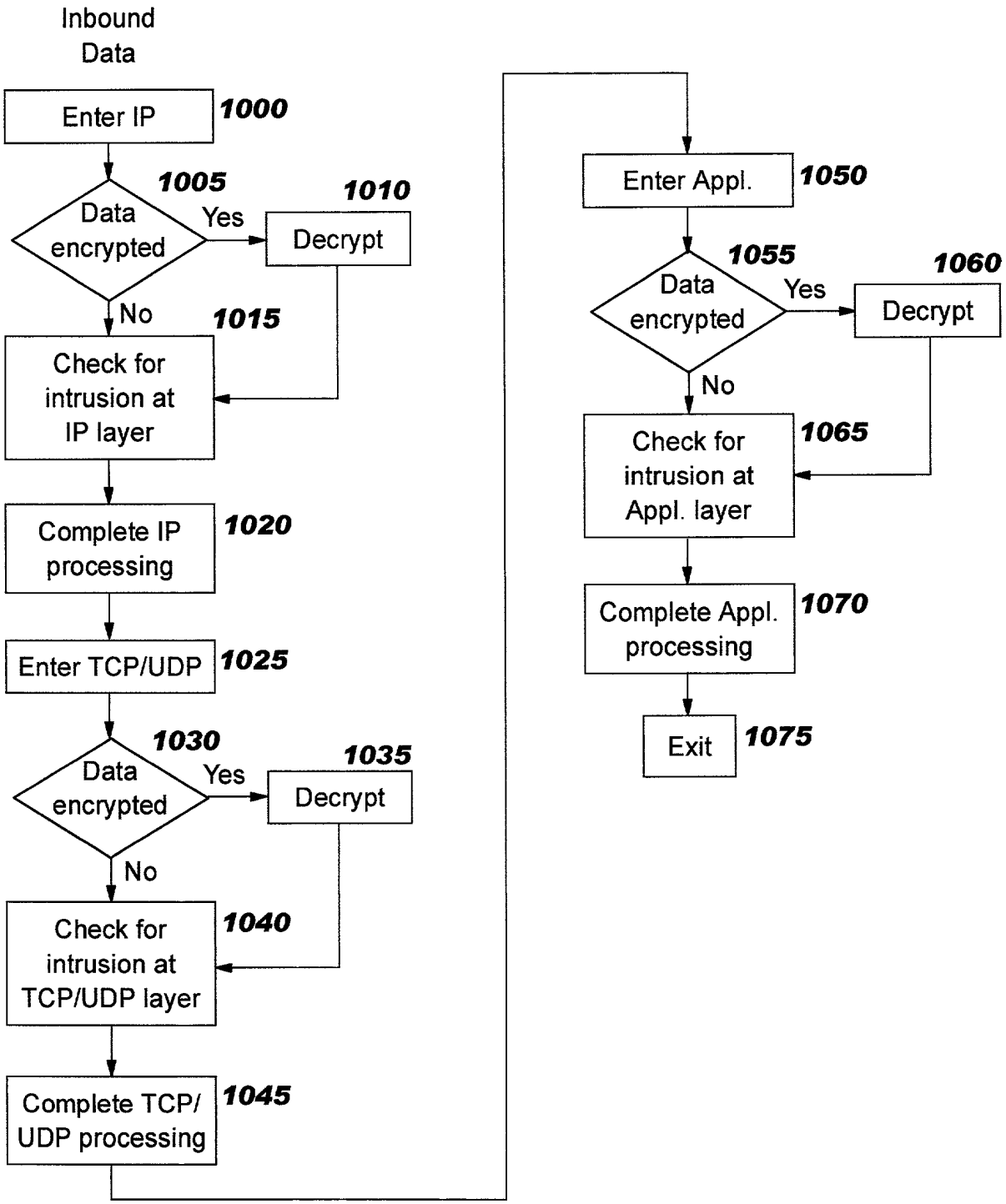

Inbound Data
Enter IP
1000
1005
Data encrypted
Yes
1010
Decrypt
No
1015
Check for intrusion at IP layer
Complete IP processing
1020
Enter TCP/UDP
1025
1030
Data encrypted
Yes
1035
Decrypt
No
Check for intrusion at TCP/UDP layer
1040
Complete TCP/ UDP processing
1045
Enter Appl.
1050
1055
Data encrypted
Yes
1060
Decrypt
No
Check for intrusion at Appl. layer
1065
Complete Appl. processing
1070
Exit
1075

FIG. 11

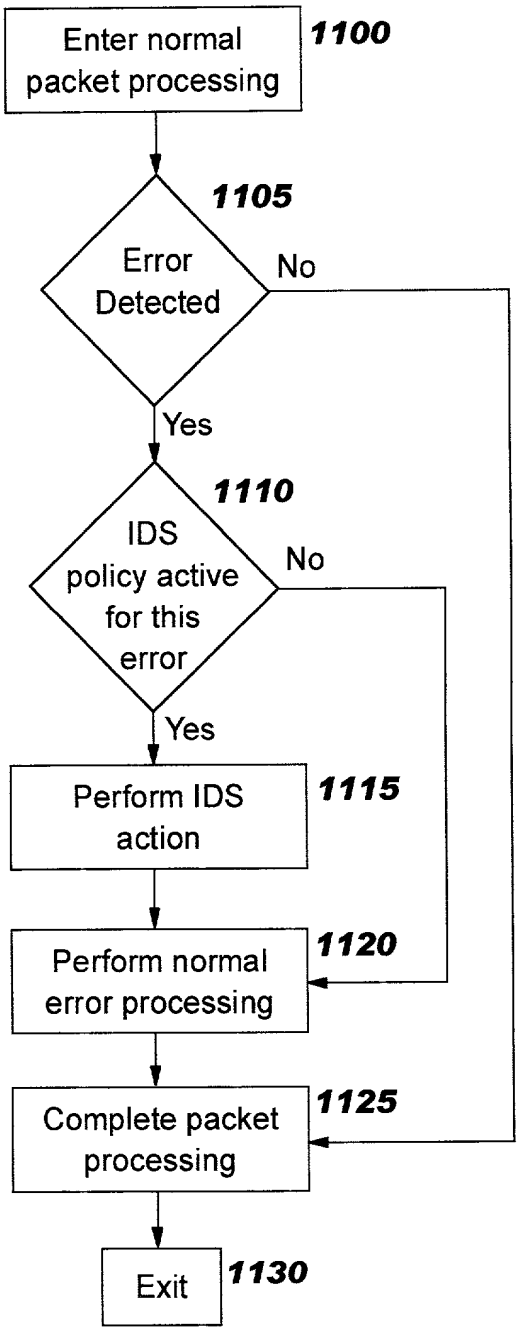

Enter normal packet processing
1100
1105
Error Detected
No
Yes
1110
IDS policy active for this error
No
Yes
Perform IDS action
1115
Perform normal error processing
1120
Complete packet processing
1125
Exit
1130

FIG. 12

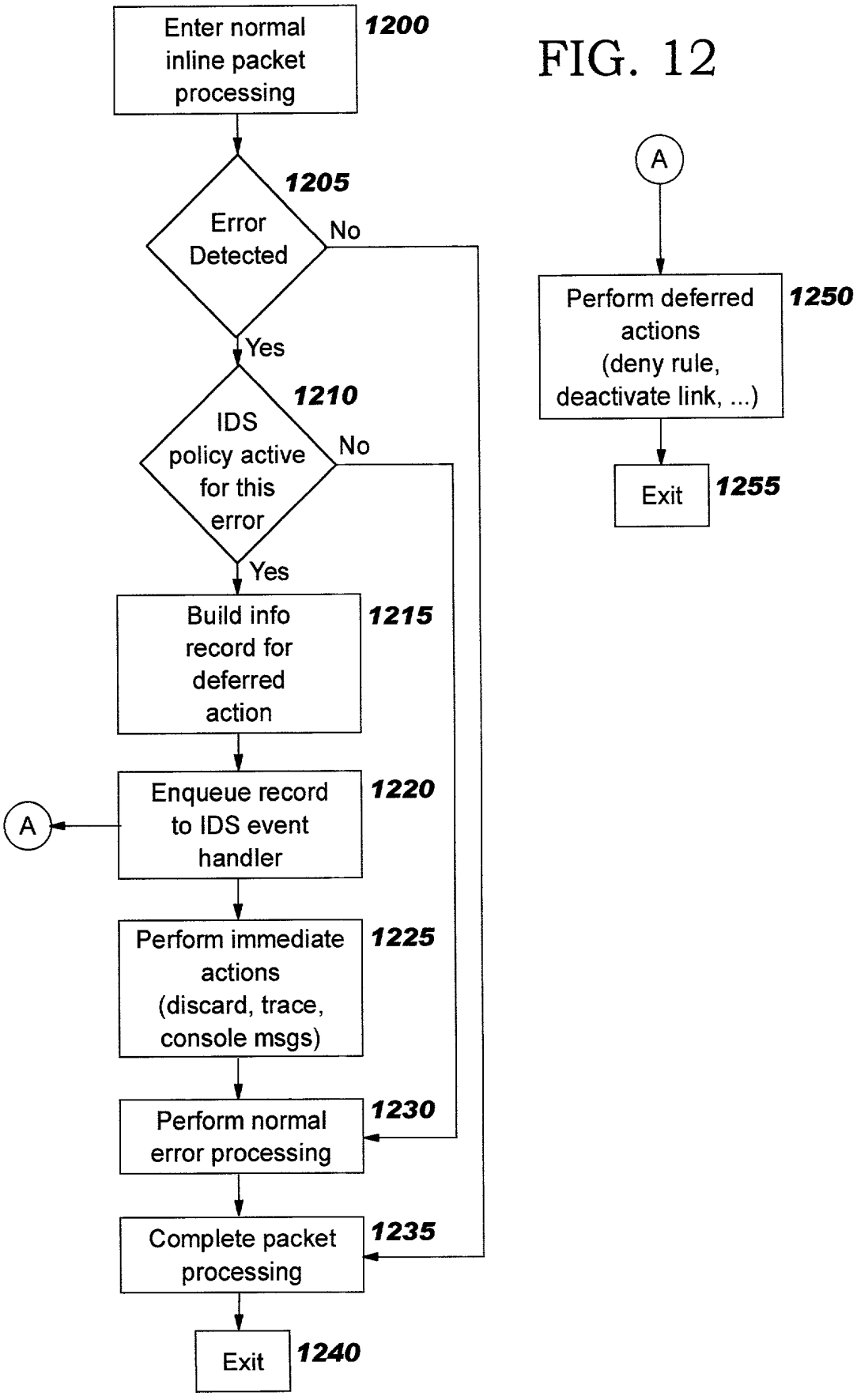

Enter normal inline packet processing
1200
Error Detected
1205
No
Yes
IDS policy active for this error
1210
No
Yes
Build info record for deferred action
1215
Enqueue record to IDS event handler
1220
A
Perform immediate actions (discard, trace, console msgs)
1225
Perform normal error processing
1230
Complete packet processing
1235
Exit
1240
A
Perform deferred actions (deny rule, deactivate link, ...)
1250
Exit
1255

FIG. 13

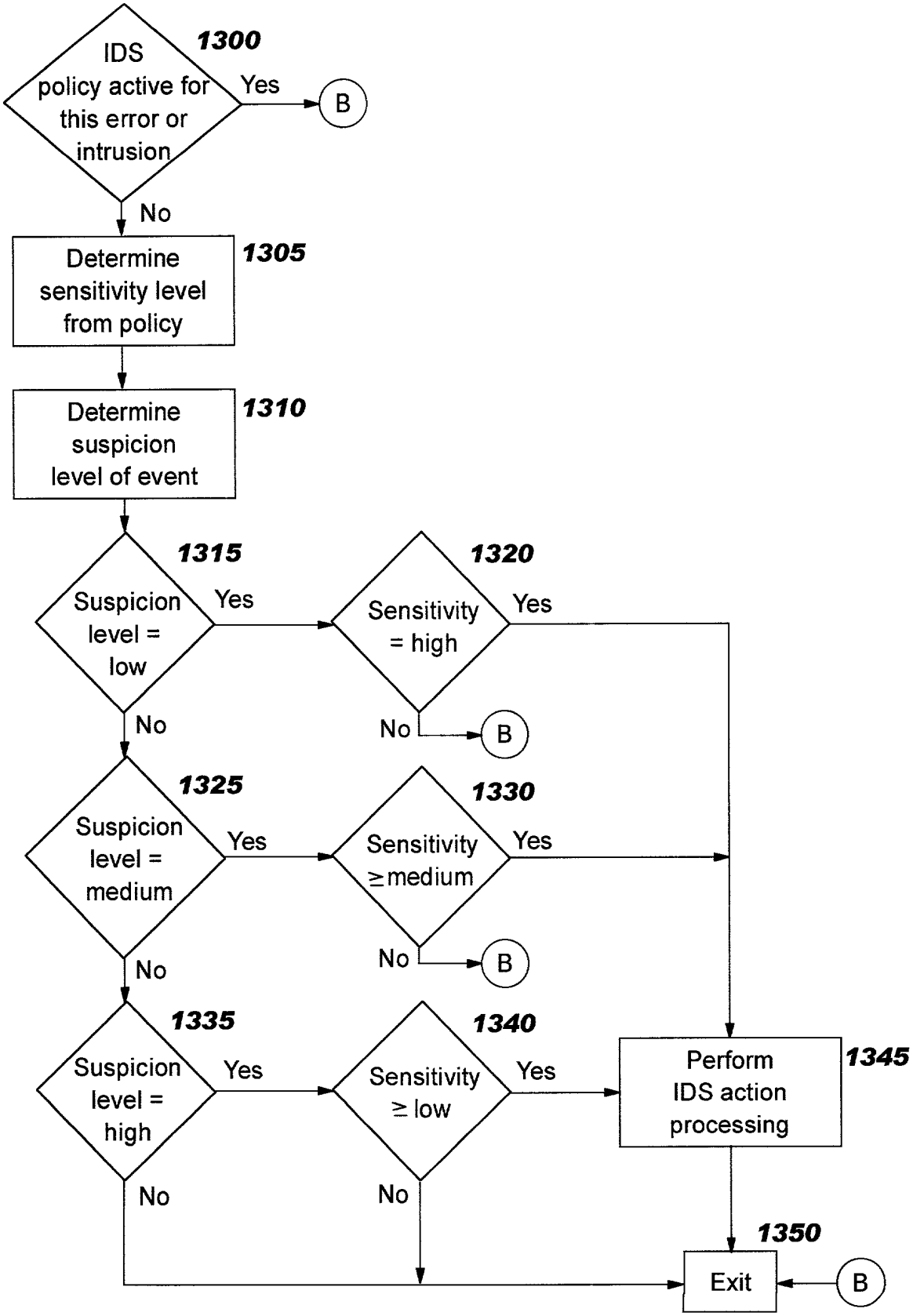

1300
IDS policy active for this error or intrusion
Yes
B
No
Determine sensitivity level from policy
1305
Determine suspicion level of event
1310
1315
Suspicion level = low
Yes
1320
Sensitivity = high
Yes
No
B
No
1325
Suspicion level = medium
Yes
1330
Sensitivity ≥ medium
Yes
No
B
No
1335
Suspicion level = high
Yes
1340
Sensitivity ≥ low
Yes
1345
Perform IDS action processing
No
No
1350
Exit
B

FIG. 14

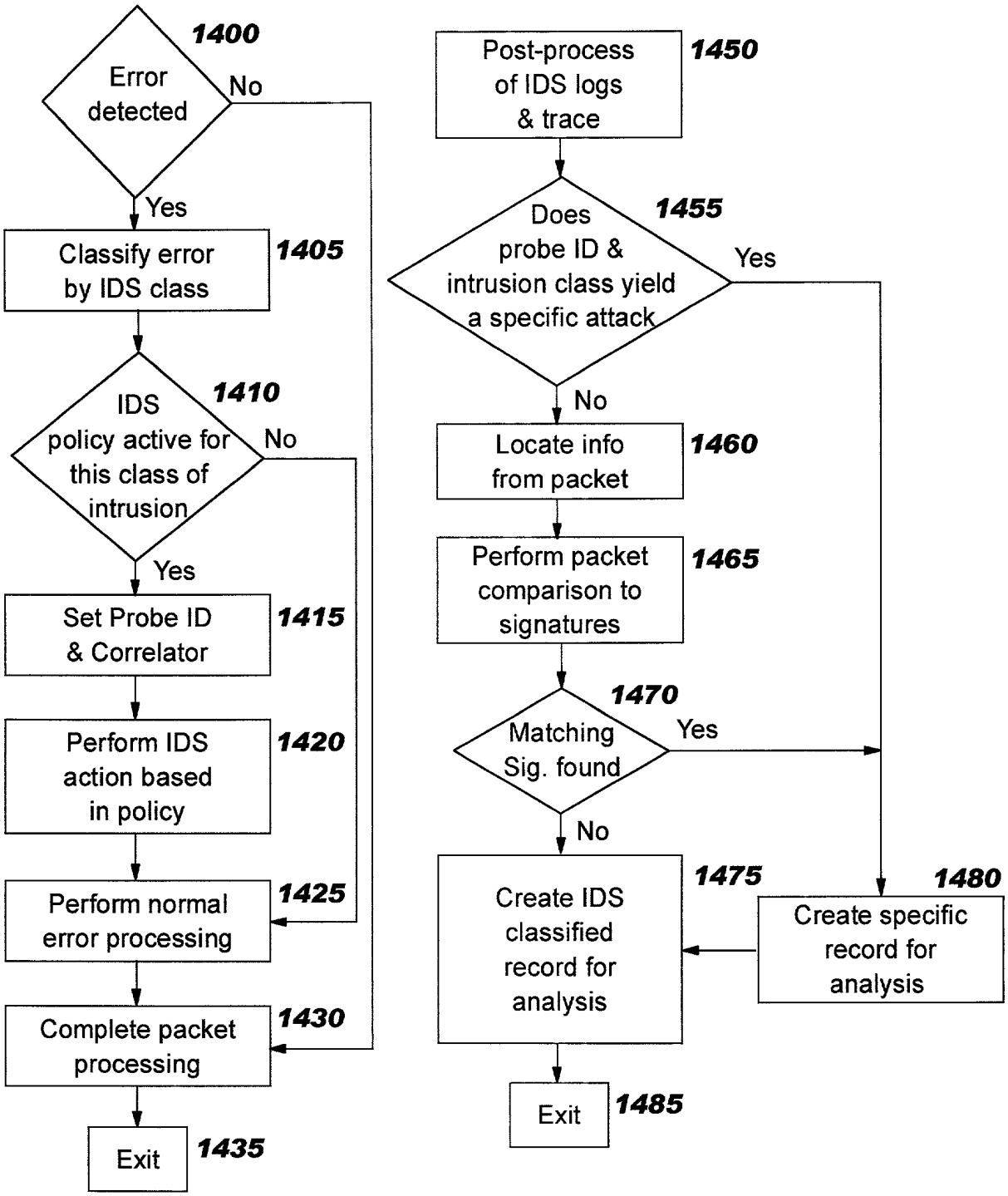

1400
Error detected
No
Yes
Classify error by IDS class
1405
IDS policy active for this class of intrusion
1410
No
Yes
Set Probe ID & Correlator
1415
Perform IDS action based in policy
1420
Perform normal error processing
1425
Complete packet processing
1430
Exit
1435
Post-process of IDS logs & trace
1450
Does probe ID & intrusion class yield a specific attack
1455
Yes
No
Locate info from packet
1460
Perform packet comparison to signatures
1465
Matching Sig. found
1470
Yes
No
Create IDS classified record for analysis
1475
Create specific record for analysis
1480
Exit
1485

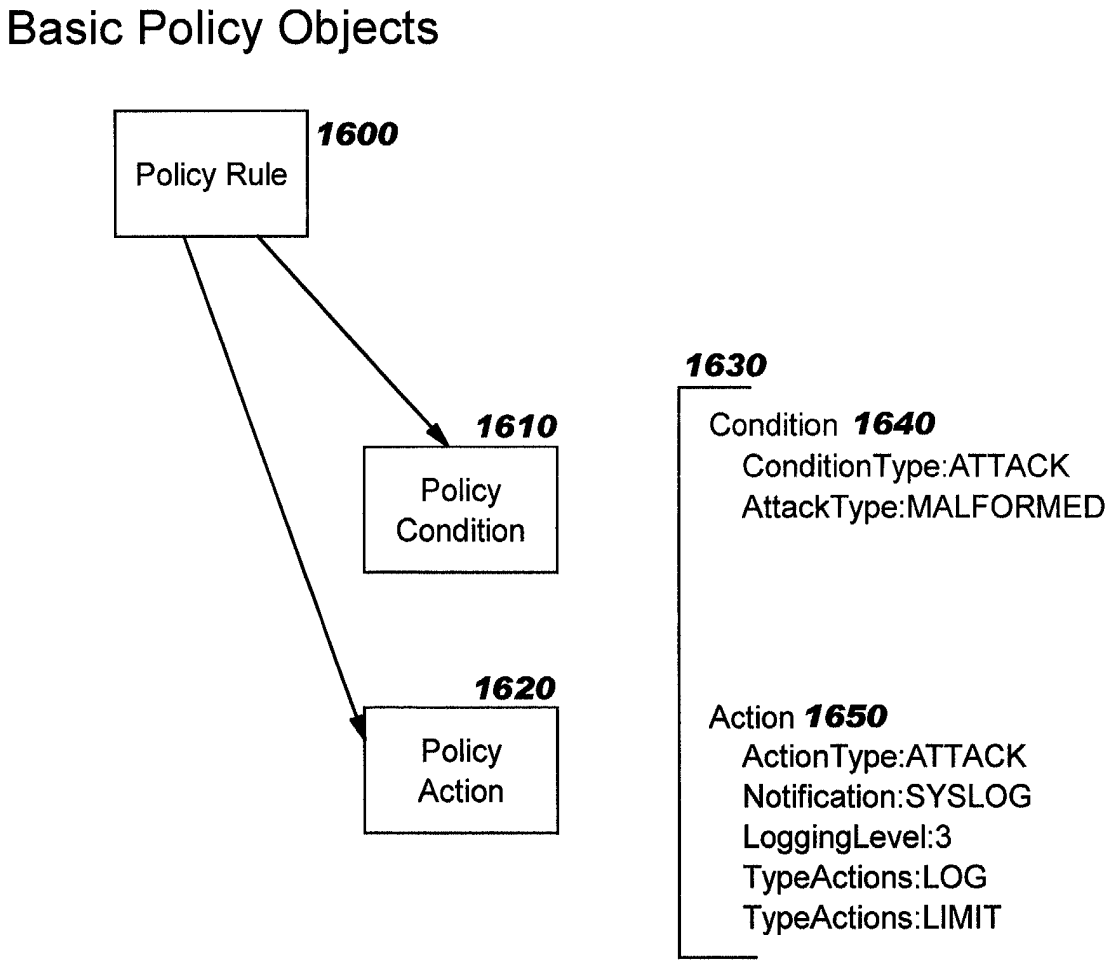
FIG. 15

1500

Sensitivity (from policy)	Low Suspicion Event (LS)	Medium Suspicion Event (MS)	High Suspicion Event (HS)
Low			Count
Medium		Count	Count
High	Count	Count	Count

1510 **1520** **1530**

FIG. 16


Basic Policy Objects
Policy Rule
1600
Policy Condition
1610
Policy Action
1620
1630
Condition 1640
ConditionType:ATTACK
AttackType:MALFORMED
Action 1650
ActionType:ATTACK
Notification:SYSLOG
LoggingLevel:3
TypeActions:LOG
TypeActions:LIMIT

1700

1710 Socket State	1720 Event	1730 Event Classification
Any state	recv unexpected flags (SYN+FIN...)	high suspicion
RESERVED	recv any packet	high suspicion
Unbound, not RESERVED	recv any packet	medium suspicion - app may be temporarily down
Listen	recv SYN	classification deferred if syn queued.
Half open connection	recv ACK	low suspicion - connection handshake completed
Half open connection	recv RST	medium suspicion - scanner covering tracks?
Half open connection	final time-out (and not syn flood)	high suspicion - scanner abandoning handshake?
Any connected state	seq# out of window	low suspicion - perhaps duplicate packet
Any connected state	recv standalone SYN	low suspicion - perhaps peer reboot
Any connected state	final time-out	medium suspicion - peer abandoned connection

1740

1750

FIG. 17

Policy Sensitivity and Event Suspicion Levels for TCP Port Scan

FIG. 18

IDS Policy Sensitivity and Event Suspicion Levels

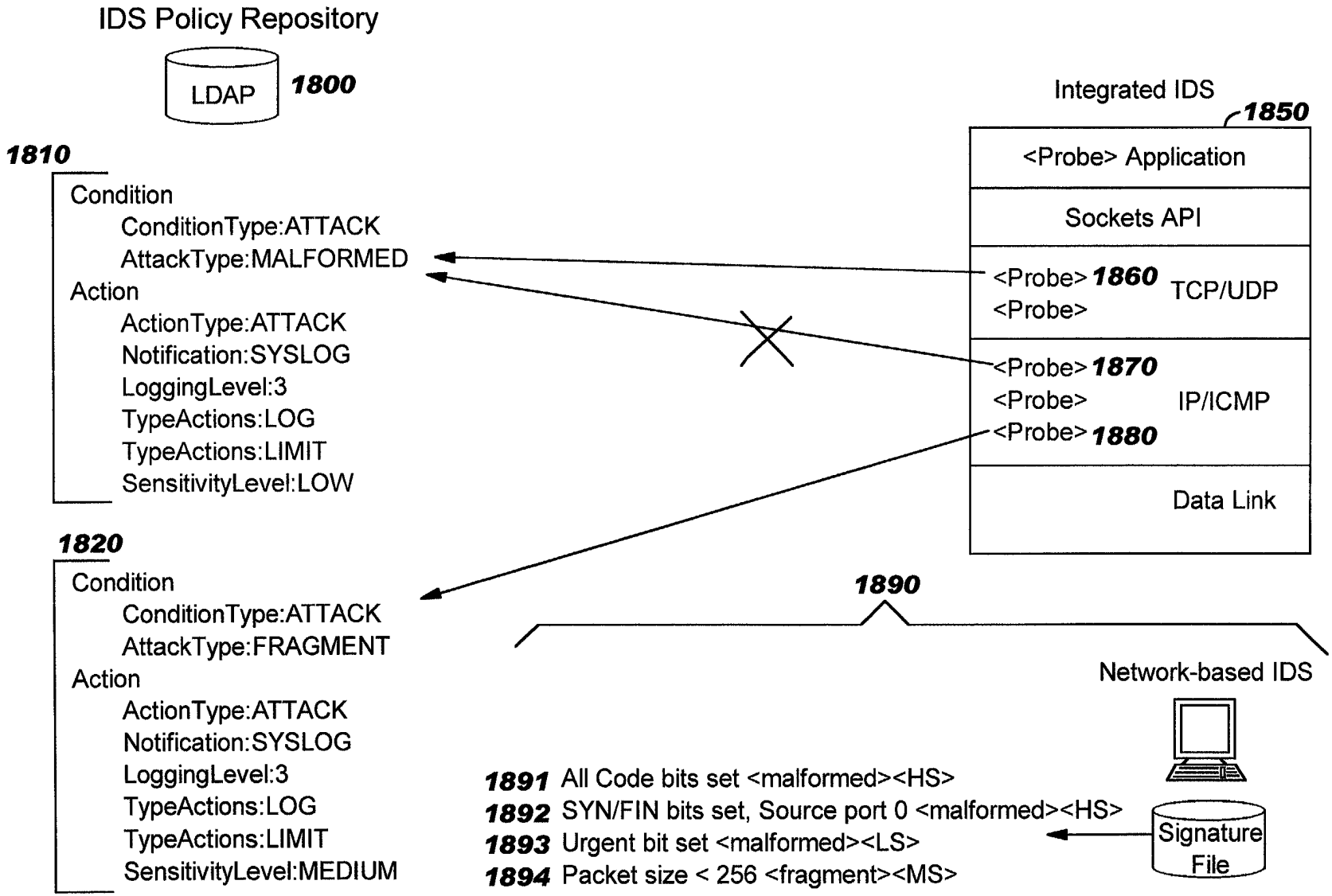


FIG. 19

Conditions and Actions - Relationship to specific attacks